

REMARKS

Status of Claims

Patent claims 1-51 of this reissue application have been cancelled.

Previously added claims 52-66, 68-74, 76-78, 85-93, 95-108 and 110-144 have been cancelled.

Previously added claims 67, 75, 79, 84, 94, 109 and 145-156 are pending.

Previously added pending independent claims 67, 75, 79, 84, 109, 145 and 154-155 are further amended by this amendment as discussed below.

New dependent claim 157 is added.

Therefore, added claims 67, 75, 79, 84, 94, 109 and 145-157 are pending.

No new matter has been added.

Rejections under 35 USC 103(a)

The Office Action rejects all pending claims under 35 USC 103(a) as being unpatentable over Cozza (US Patent No. 5,502,815), Arnold (US Patent No. 5,440,823) and Computergram International (November 28, 1989). Computergram is newly cited and newly relied upon.

The rejected independent claims are 67, 75, 79, 84, 109, 145 and 154-155. Independent claim 67 is amended, with the changes shown below relative to the previous version of claim 67 in compliance with 37 CFR 1.173 and MPEP 1453, to emphasize:

67. (six times amended) An apparatus, comprising:

a virus scanner adapted to scan a file stored in a storage device for infection with a virus;

a quarantining device adapted to quarantine the file from non-infected files on the storage device, when the file is infected; and

a converting device adapted to in response to a detection of the infection with the virus prohibit use of the infected file based upon executing an encoding process that converts the infected file into encoded data,

thereby in response to the detection of the infection with the virus, the infected file is deleted and the encoded data is stored in another storage area different from a storage area in which the infected file was stored.

For example, for support, the reissue patent FIGs. 21 and 22, S211, S224; column 18, lines

53-57; column 19, lines 46-48; and column 20, lines 51-54, discuss referring to the infection flags for an original file on the disk 30 to identify whether a file has been detected as being infected, thereby in response to the infection flags, the infected file is deleted and encoded.

The Office Action page 3 provides ‘Arnold and Cozza fail to disclose the limitation of: encoding the infected file and stored in another storage area ...’ So the Office Action relies upon Computergram.

Computergram discusses “The back-up software and hardware also automatically detect and isolate computer viruses, and compressing and encrypting them, renders them harmless.” However, Computergram discusses “the custom SDN communications software that performs the automated compression, encryption and back-up of user-specified data at user-defined intervals,” so Computergram encrypts user-specified files to be backed up, where the backup process further includes detecting viruses in the user-specified files being backed up. Therefore, in Computergram, the encrypting is in response to backing up files that have been specified by a user, which could involve encrypting a user-specified backed up file that is also infected. Computergram is silent on “a converting device adapted to **in response to a detection of the infection with the virus prohibit use of the infected file based upon executing an encoding process ... thereby in response to the detection of the infection with the virus, the infected file is deleted and the encoded data is stored in another storage area different from a storage area in which the infected file was stored.**” In other words, Computergram discusses “Once the user has defined the data to be backed up and at what time intervals,” which triggers backing up that could include detecting a virus during the backup, and then encrypting. In contrast, claim 67 emphasizes that detection of an infection triggers encoding.

Computergram discusses “isolate computer viruses,” however, Computergram does not teach how the isolation is achieved, namely by “**in response to the detection of the infection with the virus, the infected file is deleted ... and ...stored in another storage area different from a storage area in which the infected file was stored.**”

In addition, the Office Action page 3 acknowledges that Arnold does not disclose ‘storing a detected virus infected file into a specific area,’ so the Office Action relies upon Cozza, however, Cozza only discusses storing initial state information for detecting a virus in a cache.

A benefit is that in response to a detection of an infection with a virus, use of the infected file is prohibited via an encoded, quarantined and deleted infected file, which is patentably distinguishing over Arnold, Cozza and Computergram. For example, the reissue patent

specification column 15, lines 9-11, column 20, lines 51-61, FIG. 22 (e.g., S224) and column 19, lines 48-54 provide support.

The rejection of claim 67 can be withdrawn.

Independent claims 75, 79, 84, 109, 145 and 154-155 are amended to emphasize features similar to the discussed features of amended claim 67, and the changes in relation to the previous version of the claims are shown in compliance with 37 CFR 1.173 and MPEP 1453 as follows:

75. (six times amended) An apparatus comprising:

- a storage device adapted to store a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

- a virus checking device adapted to select a file to be checked for infection with a virus;

- a quarantining device adapted to quarantine an infected file on the storage device; and

- a converting device adapted to in response to a detection of the infection with the virus prohibit use of the infected file based upon executing an encoding process for security that converts the infected file into encoded data,

- thereby in response to the detection of the infection with the virus, the infected file is deleted and the encoded data is stored in another storage area different from a storage area in which the infected file was stored.

79. (six times amended) An apparatus, comprising:

- a storage device adapted to store a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

- a virus checking device adapted for selection of a file to be checked for infection with a virus; and

- a converting device adapted to in response to a detection of the infection with the virus prohibit use of an infected file based upon executing an encoding process for security that converts the infected file into encoded data,

- thereby in response to the detection of the infection with the virus, the infected file is deleted and the encoded data is stored in another storage area different from a storage area in which the infected file was stored.

84. (six times amended) A method, comprising:

- scanning a file for infection with a virus using a computer;

quarantining the file from non-infected files if the file is infected with a virus; and

in response to a detection of the infection with the virus prohibiting use of the infected file by executing an encoding process for security that converts the infected file into encoded data,

thereby in response to the detection of the infection with the virus, the infected file is deleted and the encoded data is stored in another storage area different from a storage area in which the infected file was stored.

109. (six times amended) A method comprising:

scanning a file for infection with a virus using a computer;

isolating the file from non-infected files, if the file is infected with a virus; and

in response to a detection of the infection with the virus prohibiting use of the infected file via executing an encoding process for security that converts the infected file into encoded data,

thereby in response to the detection of the infection with the virus, the infected file is deleted and the encoded data is stored in another storage area different from a storage area in which the infected file was stored.

145. (three times amended) A method for performing an anti-virus operation, the method comprising:

detecting a virus-infected file in a storage device using a computer;

in response to the detection of the virus-infected file prohibiting use of the virus-infected file based upon converting for security the virus-infected file into encoded data; and

storing the encoded data of the virus-infected file,

thereby in response to the detection of the virus-infected file, the virus-infected file is deleted and the encoded data is stored in another storage area different from a storage area in which the virus-infected file was stored.

154. (twice amended) A method for performing an anti-virus operation, the method comprising:

detecting a virus-infected file using a computer;

in response to the detection of the virus-infected file prohibiting use of the virus-infected file by encoding the virus-infected file for security; and

storing the encoded virus infected file,

thereby in response to the detection of the virus-infected file, the virus-infected file is deleted and the encoded data is stored in another storage area different from a storage area in which the virus-infected file was stored.

155. (twice amended) A method for performing an anti-virus operation, the method comprising:

detecting a virus-infected file in a storage device using a computer;

in response to the detection of the virus-infected file
converting for security the virus-infected file into encoded data; and
storing the encoded data of the virus infected file,

thereby in response to the detection of the virus-infected file, the virus-infected file is deleted and the encoded data is stored in another storage area different from a storage area in which the virus-infected file was stored and the converting into the encoded data prohibits use of the virus-infected file.

New Dependent Claim 157

In contrast to Arnold, Cozza and Computergram, new claim 157 emphasizes “wherein the other storage area as a quarantine is an inexecutable area that is protected.” For example, reissue patent column 13, line 66 to column 14, line 5, provides support.

The remaining dependent claims inherit the patentable recitations of their respective base claims, and therefore, patentably distinguish over the cited art for the reasons discussed above in addition to the additional features recited therein.

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance.

If there are any matters remaining after this response, Applicants respectfully request the Examiner to telephone the undersigned to attend to these matters to expedite prosecution.

Serial No. 09/893,445

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,
STAAS & HALSEY LLP

/Mehdi D. Sheikerz/

Date: _____ June 6, 2011 _____

By: _____
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501